(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 July 2001 (19.07.2001)

PCT

(10) International Publication Number
WO 01/52543 A1

(51) International Patent Classification[7]: H04N 7/167

(21) International Application Number: PCT/US01/01173

(22) International Filing Date: 12 January 2001 (12.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/483,066 14 January 2000 (14.01.2000) US

(71) Applicant: DIVA SYSTEMS CORPORATION [US/US]; 800 Saginaw Drive, Redwood City, CA 94063 (US).

(72) Inventor: BERTRAM, Michael, C.; 417-17 Camille Circle, San Jose, CA 95134 (US).

(74) Agents: SUEOKA, Greg, T. et al.; Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306 (US).

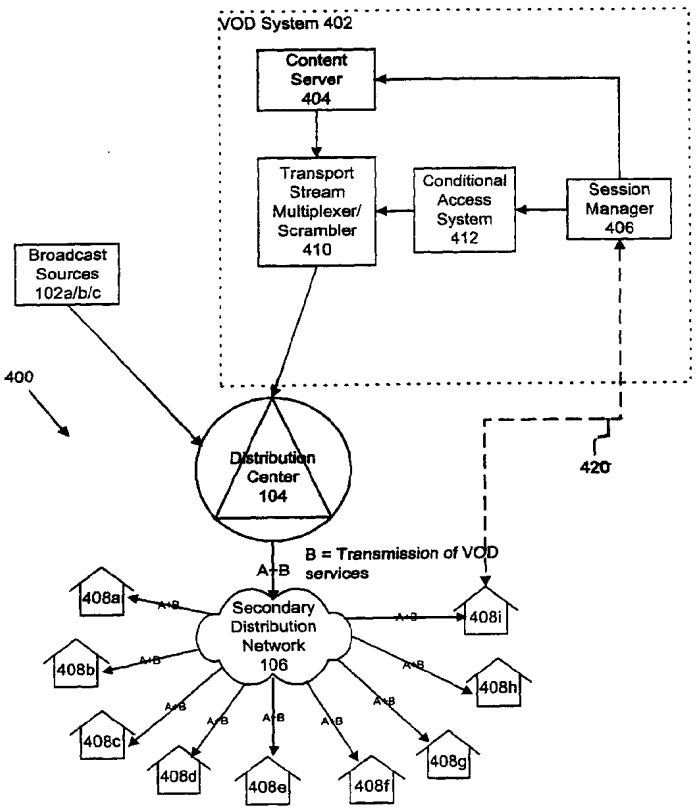
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: CONDITIONAL ACCESS AND SECURITY FOR VIDEO ON-DEMAND SYSTEMS



(57) Abstract: A system that provides secure transmission and complete access control for target devices. Such a system includes a distribution center, a video-on-demand system, a transmission network and a plurality of target devices. The video-on-demand system advantageously provides for encryption of the transmission, transmission of access keys, and access control. The target devices also include circuitry for communicating with the video server and decrypting the transmission and controlling access to video services. A method for providing conditional access to video services for a plurality of subscriber stations comprises the steps of: authorizing the plurality of subscriber stations to receive the video services; receiving a first order for a first video service from a first subscriber station; and transmitting tuning data to the first subscriber station so that the first subscriber station is able to receive the first video service. The method may also prevent the theft of the content of transmissions by performing the steps of: scrambling the first video service using a first key to generate a first scrambled video service; scrambling the first key using decryption data to generate a first scrambled key; distributing the decryption data to decrypt the first scrambled key to the plurality of subscriber stations; transmitting the first scrambled video service to the plurality of subscriber stations; and transmitting the first scrambled key to the plurality of subscriber stations.

WO 01/52543 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONDITIONAL ACCESS AND SECURITY FOR VIDEO ON-DEMAND SYSTEMS

Inventor: Michael C. Bertram

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to the field of video distribution networks. In particular, this invention relates to conditional access and security for video on-demand distribution networks.

2. Description of the Background Art

Conditional access for digitally transmitted services satisfies at least two important goals. First, it protects the content from theft during transmission.. Second, it provides specific controls over which target devices may access and use the content.

Three major digital video conditional access approaches currently exist in the marketplace. The GI Digicypher system from General Instruments and the SA Powerkey system from Scientific-Atlanta are used for digital broadcast services, primarily in the United States. DVB Common Scrambling Algorithm based systems are used primarily in Europe.

Current practice for conditional access for digital broadcast services works well because of several attributes of broadcast services. These attributes include: 1) that digital broadcast services are usually comprised of a fairly small number of data streams (on the order of tens); 2) that digital broadcast services have many potential users of each data stream; and 3) that digital broadcast services can generally be pre-scheduled (this is true of both premium services and pay per view services) allowing authorization to be generated and distributed before they are needed.

However, the current practice for conditional access for digital broadcast services does not work well for video on-demand services and systems. Video on-demand services have attributes which are quite different from the attributes of digital broadcast services. Problematic attributes of video on-demand services for conditional access systems include: 1) that video on-demand services use a large number of data streams (on the order of thousands); 2) that video on-demand services target data streams to individual users; and 3) that video on-demand services are not pre-scheduled.

Although the current practice for conditional access for digital broadcast services can be applied to video on-demand services, the different attributes discussed above lead to problems. For example, the current practices for conditional access typically are not designed to accommodate the generation and distribution of encryption keys and authorizations for thousands of services. Additionally, the generation and distribution time for on-demand authorizations is not fast enough to support timely decryption of video on-demand services.

Therefore, there is a need for conditional access systems and methods for video on-demand services that protects the content from theft and controls access of target devices to the content.

SUMMARY OF THE INVENTION

The present invention overcomes the shortcomings of the prior art and provides a solution to the conditional access and security issues presented above. In accordance with the present invention, a method for providing conditional access to video services for a plurality of subscriber stations comprises the steps of: authorizing the plurality of subscriber stations to receive the video services; receiving a first order for a first video service from a first subscriber station; and transmitting tuning data to the first subscriber station so that the first subscriber station is able to receive the first video service. In another aspect, the present invention is also directed to preventing theft of the content of transmissions with a method comprising the additional steps of: scrambling the first video service using a first key to generate a first scrambled video service; generating a de-scrambling message having scrambling data to allow de-scrambling of the first video service by the plurality of subscriber stations; transmitting the first scrambled video service to the plurality of subscriber stations; and transmitting the de-scrambling message to the plurality of subscriber stations.

The present invention also includes a system that provides secure transmission and complete access control for target devices. Such a system includes a distribution center, a video-on-demand system, a transmission network and a plurality of target devices or subscriber stations. The video-on-demand system advantageously provides for scrambling of the transmission, transmission of de-scrambling messages, and access control. The target devices also include circuitry for communicating with the video server and de-scrambling the transmission and controlling access to video services.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic diagram of a conventional video broadcast distribution network.

Figure 2 is a flow chart of the prior art method for processing of the content at the distribution center and transmission to subscriber stations.

Figure 3A is a flow chart of the prior art method for receiving and processing a transmission at an authorized subscriber station.

Figure 3B is a flow chart of the prior art method for receiving and processing a transmission at an unauthorized subscriber station.

Figure 4A is a schematic diagram of a video-on-demand system utilizing the present invention.

Figure 4B is a block diagram of a subscriber station in the system of Figure 4A.

Figure 5 is a flow chart of a preferred embodiment of the method for processing of the content at the distribution center and transmission to subscriber stations.

Figure 6A is a flow chart of a preferred embodiment of the method for receiving and processing a transmission at a subscriber station that has requested video-on-demand services.

Figure 6B is a flow chart of a preferred embodiment of the method for receiving and processing a transmission at an subscriber station that has not requested video-on-demand services.

Figure 6C is a flow chart of a method for receiving and processing a transmission at a non-subscriber station attempting to pirate video-on-demand services.

Figure 7 is a block diagram illustrating the transmission of data and keys with respect to time according to the prior art.

Figure 8 is a block diagram illustrating the transmission of data and keys with respect to time according to the present invention.

Figure 9 is a block diagram illustrating a hybrid/fiber coax network and the use of keys per channel and program according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Throughout this description various terms are used to describe the invention. Unless modified by the following description, several of the terms are defined as follows: Scrambling comprises a method of protecting a data stream by transforming the value bits in the stream based on a given key. For the purposes of this disclosure, scrambling has the same meaning as encrypting. De-scrambling comprises a method of transforming data stream bits back to their original value based on the use of a key. For the purposes of this description, de-scrambling has the same meaning as decryption. A conditional access (CA) system is a system that generates keys, de-scrambling messages, and authorization messages supporting the scrambling and de-scrambling of, e.g., MPEG encoded programs. A de-scrambling message comprises a conditional access message containing de-scrambling information for a particular MPEG program. The de-scrambling information may be the de-scrambling key or the information a Set Top Box (or boxes) needs to generate or derive the de-scrambling key. An authorization message comprises a conditional access message authorizing a particular Set Top Box to use a de-scrambling key to de-scramble a particular MPEG program.

Figure 1 is a schematic diagram of a conventional video broadcast network 100. The conventional video broadcast distribution network 100 typically includes one or more broadcast sources 102a, 102b, and 102c, one or more distribution centers 104, one or more secondary distribution networks 106, and a plurality of targets or subscriber stations 108a-i.

The broadcast sources 102a, 102b, and 102c provided video and audio content for various channels in the broadcast network 100. For example, the broadcast sources 102a, 102b, and 102c include what are referred to as premium channels such as HBO, Showtime, Cinemax, etc. The sources 102a, 102b, and 102c may also be, for example, pay-per-view (PPV) channels. The sources 102a, 102b, and 102c are typically coupled via a primary distribution network (show as connector lines) to the distribution center 104.

The distribution center 104 may be, for example, a cable head-end. The distribution center 104 receives the content from the broadcast sources 102a, 102b, 102c, and associates the content with channels and transmits the content over predetermined channels in the secondary distribution network 106. The distribution center 104 is coupled via a secondary distribution network 106 to the subscriber stations 108a-i. The secondary distribution network 106 comprises for example, various amplifiers, bridges, taps, and drop cables.

Finally, the subscriber stations 108a-i may be, for example, set-top boxes and associated television equipment for viewing the video content by end users.

Referring now to Figure 2, the prior art method for preventing theft of the transmission data is shown. The cable distribution networks 100 of the prior art prevents theft by scrambling the signals before transmission. Figure 2 illustrates the processing of the video and audio signals (content) done at the distribution center 104 before transmission. In the prior art, the distribution center 104 sends or distributes authorization for pre-scheduled services to the individual subscriber stations 108 in step 202. Then at some later time, the distribution center 104 scrambles a pre-scheduled service in step 206 and at the same time generates a de-scrambling message in step 208. Next in step 210, the distribution center 104 sends the scrambled pre-scheduled service and the de-scrambling message over the network 106.

Referring now to Figures 3A and 3B, the prior art method for processing the scrambled data at the subscriber stations 108a-i will be described. Figure 3A shows the prior art method for receiving and processing a transmission at an authorized subscriber station 108a-i. In contrast, Figure 3B, shows the prior art method for receiving and processing a transmission at an unauthorized subscriber. These are the two general processing scenarios at the subscriber stations 108a-i provided with the prior art.

Referring now to Figure 3A, the processing at the subscriber station 108 begins in step 302 where the subscriber station 108 receives an authorization for pre-scheduled service over the secondary distribution network 206 from the distribution center 104. Parallel in time to, or even before or after step 302, the user inputs signals to a corresponding subscriber station 108 to tune the subscriber station 108 to the pre-scheduled service in step 306. Then in step 308, the subscriber station 108 receives the scrambled data for pre-scheduled service and a de-scrambling message. Once steps 302, 306, and 308 have been completed, the prior art process transitions to step 310. Now having received the necessary information from steps 302 and 308, the subscriber station 108 generates or derives the key using the de-scrambling message from step 308 if authorized. Next in step 312, the subscriber station 108 de-scrambles the pre-scheduled service using the derived key from step 310. Having de-scrambled the signal, the subscriber station 108 can display the pre-scheduled service on a display device of the subscriber station 108. As has been noted above, the key is used to control access by the respective subscriber station 108 to the content. Thus, a unique key is needed for each program, and each subscriber station 108a-I

must receive the authorization before the key to the program can be decrypted in the prior art.

Referring now to Figure 3B, the processing that occurs when an unauthorized subscriber station 108 attempts to gain access to the content is illustrated. Figure 3B is a flow chart of the prior art method for receiving and processing a transmission at an unauthorized subscriber station. For ease of understanding like reference numerals have been used for like steps. Similar to the authorized case, the user inputs signals to a corresponding subscriber station 108 to tune the subscriber station 108 to the pre-scheduled service in step 306. Also in step 308, the subscriber station 108 receives the scrambled data for pre-scheduled service and the de-scrambling message. However, step 302 at the unauthorized subscriber station 108 are never completed. Rather as shown by the flow chart in step 316 the subscriber station 108 does not receive the authorization for pre-scheduled services. Therefore, the unauthorized subscriber station 108 is unable to perform step 310 and is unable to derive the key and de-scramble the signal for display in step 320. Thus, Figures 3A and 3B show the importance in the prior art of having a fairly small number of data streams (on the order of tens) that have many potential users, and that digital broadcast services can generally be pre-scheduled allowing authorization to be generated and distributed before they are needed.

Figure 4 is a schematic diagram of a system 400 utilizing the present invention. The present invention is directed to the addition of a video-on-demand system 402 and to providing conditional access and security in such a combined system 400. Again, for ease of understanding like reference numerals have been used for similar elements with the same functionality. The combined system 400 preferably comprises one or more broadcast sources 102a/b/c, one or more video-on-demand (VOD) system 402, a distribution center 104, a VOD content server 404, a session manager 406, a transport multiplexer 410, a conditional access system, a secondary distribution network 106 and a plurality of subscriber stations 408a-408i. An exemplary such video-on-demand system 400 is described in pending U.S. Patent Application Number 08/984,710, filed December 4, 1997, and entitled "System for Interactively Distributing Information Services," the disclosure of which is incorporated herein by reference. The following description will focus on differences from such a system.

As noted above, the combined system 400 differs from the prior art of Figure 1 by providing video-on-demand data streams. To provide such functionality, the system 400

has a plurality of VOD systems 402 to provide the content as requested by the subscriber stations 108a-108i in addition to the broadcast sources 102 used in traditional cable networks to provided video and audio content for various channels. The VOD system 402 for example may include various movies that may be requested by the user. The available number of movies to the subscriber stations 108a-108i can be in the thousands. Both the broadcast sources 102 and the VOD system 402 are coupled to provide their content to the distribution center 104, preferably via a primary distribution network.

The VOD system 402 preferably comprises a content server 404, a session manager 406, a transport stream multiplexer/scrambler 410 and a conditional access system 412. The content server 404 stores the video content such thousands of movies, and in response to signals from the session manager 406 provides the video content to the transport stream multiplexer/scrambler 410. The session manager 406 controls the content server 404, the transport stream multiplexer/scrambler 410 and the conditional access system 412 in response to user requests. The session manager is coupled to each of these devices for sending control signals. The session manager 406 is also coupled to each subscriber station 408 by a out of band communication channel 420 to receive input from the subscribers. Although only one such path is shown in Figure 4A, it should be understood there is such a coupling for each subscriber station 408a-i. In response to signals from the session manager 406, the conditional access system 412 sends control signals, encryption keys and authorization messages to the transport stream multiplexer/scrambler 410. As will be known to those skilled in the art, multiple commercial vendors offer conditional access systems compatible with conditional access messaging defined by the MPEG-2 standard that could be used for conditional access system 412. The transport stream multiplexer/scrambler 410 send the content and control signal in both scrambled and not scrambled format to the distribution center 104. The session manager 406 also instructs the transport stream multiplexer/scrambler 410 which channels and program ID to use when transmitting the content.

The distribution center 104 is similar to that described above with reference to Figure 1. The distribution center 104 transmits the typical broadcast content, but also transmits the content, access and communication necessary for VOD services. For example, the VOD system 402 may provide the functionality as described in U.S. Patent Application Serial No. 08/984,710, filed December 4, 1997, entitled "System for Interactively

Distributing Information Service" which is incorporated herein by reference. The distribution center 104 is coupled to the secondary distribution network 106. Those skilled in the art will recognize that distribution center 104 of the present invention differs from the prior art in the following respects. First, the streams transmitted include both the typical broadcast content (A) but also video-on-demand services (B) as shown in the Figure 4. Second, the coupling of the distribution center 104 to the secondary distribution network 106 provides a return channel (shown by dotted line 420) for sending signals from the subscriber stations 408a-i to the VOD system 402, in particular, the session manager 406. Third, the VOD services are provided on channel resources that are re-used and reallocated to different subscribers, and the subscriber station requires tuning information to access the VOD services. Finally, that there is processing by the VOD system 402, and communication between the VOD system 402 and the subscriber stations 408, as will be described above with reference to Figures 5-6C, to enforce transmission security and access.

The distribution center 104 and the VOD system 402 are coupled via a secondary distribution network 106 to the subscriber stations 408a-408i. The secondary distribution network 106 comprises for example, various amplifiers, bridges, taps, and drop cables. The subscriber stations 408a-408i are, by way of example, set-top boxes and associated television equipment for viewing the video content by end users. In the present invention, the subscriber stations 408a-408i or set-top boxes differ from the prior art in that they included added functionality in the form of programs downloaded or stored in ROM that provide the functionality described below with reference to Figures 6A-6C. More specifically, the programs provide method for ensuring that access to the VOD services are authorized and that does not suffer from the above-identified shortcomings of the prior art. Referring now to Figure 4B, one exemplary embodiment for a subscriber stations 408 is shown. Each subscriber station 408 preferably comprises a tuner/de-multiplexer 450, a controller 452, a de-scrambler 454, a key generator 456, a video decoder 457, and a display device 458. Basically, the tuner/de-multiplexer 450 tunes to a particular frequency and program ID in response to signals from the controller 452. The tuner/de-multiplexer 450 monitors the channels and extracts the signals for the identified channel. The tuner/de-multiplexer 450 also extracts control information from the channel and provides it to the controller 452 and the key generator 456. General control signals, tuning information, and other communication with the session manager 406 are provided to the controller 452. . The tuner/de-multiplexer 450 also extracts and provides entitlement management messages

and entitlement control messages to the key generator 456. For example, the key generator 456 may be a smart card coupled to the subscriber station 408 or may be ROM included in the subscriber station 408. Using the EMMs and the ECMs, the controller 452 enables the key generator 456 to derive a key that is sent to the de-scrambler 454 to de-scramble or decrypt the video content. Once de-scrambled, the video streams are presented to the video decoder 457 that converts the MPEG streams to an video analog signals. The analog signals are then presented to a display device 458.

It should be noted that while the methods of the present invention will now be discussed in the context of a video distribution system for cable networks, the present invention is applicable to any variety of video distribution system whether is uses cable or some other media for distribution such as but not limited to a satellite system, a digital subscriber line system, and a microwave system.

Referring now to Figure 5, a preferred embodiment of the method for processing of the content at the distribution center 104 and transmission of the content to subscriber stations 408 according to the present invention is shown. The method begins in step 501 by configuring the conditional access system 412 to scramble all the VOD programs as scrambled broadcast services. In other words, the VOD services are provisioned to be scrambled all the time. This is preferably done prior to the authorization of any subscribers to the VOD services. The programs are also scrambled independent of any particular content carried on the VOD streams. This is particularly advantageous because it addresses the problem that the VOD services are not pre-scheduled. Next in step 502 at least one subscriber station 408 is authorized for all VOD services. More preferably, the present invention authorizes all subscriber stations 408 connected to the network for all VOD services. This authorization is preferably accomplished by having the server 404 send the authorization to the all subscriber stations 408. An authorization message is a message authorizing a particular subscriber station to use a de-scrambling key to de-scramble a program. More specifically, authorization of the subscriber stations 408 is performed by sending an entitlement management message (EMM) from the distribution center 104 to each of the subscriber stations 408. This step 502 is preferably performed at initialization of the communication between a particular subscriber station 408 and the system 400.

At some later point in time after step 502 has been performed, the method proceeds in parallel to steps 512, 506, 508. Since the system 400 provides the streams of video data in response to a request from respective subscriber station 408. The duration between step

502 and the other steps 512, 506, 508 can vary significantly for each subscriber station 408 and may be any length of time. In step 512, using the return channel unique to the VOD system 400, the VOD system 402 and distribution center 104 receives a request or order for VOD services from a particular subscriber station 408. Next in step 514, responsive to the request, the VOD system 402 and distribution center 104 sends tuning data to the individual subscriber 408. This preferably accomplished by sending the frequency and MPEG program number by reference or value using the VOD downstream communication control path. The actual information for tuning to the channel may be provided or this virtually may be done by providing a index to a table at the subscriber station 408 that is used to look up the value in a table. This feature of the present invention is particularly advantageous because it solves the problem presented VOD services of targeting data streams to individual users. In broadcast systems, the tuning information is know by the user, can be used to tune to the program and cannot be used to control access. However, in the present invention, since different program streams are targeted to different users, the transmission and use of the tuning information as described above permits the targeting of particular programs streams to particular users as was not possible in the prior art. In step 506, the VOD system 402 and distribution center 104 scrambles or encrypts the streams of the VOD service; and in step 508, the VOD system 402 and distribution center 104 generate a de-scrambling message for producing the key for decoding the streams of the VOD service. The de-scrambling message preferably includes data that can be used by the subscriber station 408 to derive or generate the key. The de-scrambling message preferably takes the form of an entitlement control message (ECM) in the MPEG protocol. The present invention preferably uses the same key or key set for a number of programs. Then in step 510, the distribution center 104 transmits the scrambled VOD service and the de-scrambling message over the secondary distribution network 106. This completes the processes of the present invention at the distribution center 104. As has been described above, the security of the content being distributed is maintained by the present invention using scrambling or encryption. Any one of the various and conventional encryption methods could be used. It should be noted the present invention is particularly advantageous because the system 400 uses the same keys for all subscriber stations 408. Thus, even with thousands of subscribers, the distribution of the keys is not problematic. In other words, the keys are used to protect against theft of the transmission signal but are not use to control or prevent access by a subscriber station 408. While the present invention uses multiple keys for

groups of subscribers, the present invention avoids the problem of the prior art of requiring a key for each subscriber station 408 connected to the network 106.

Referring now to Figures 6A-6C, the various processes that may occur at the subscriber stations 408 will be described. With the method of the present invention, there are three possible scenarios: an authorized user ordering VOD service, a subscriber not ordering VOD service, an attempt to pirate or steal VOD service.

Referring particularly to Figure 6A, the preferred method for receiving and processing a transmission at a subscriber station 408 that has requested video-on-demand services will be described. The process begins in step 608 with the user inputting an order for VOD services, and the respective subscriber station 408 receiving input and generating an order for VOD services that is sent over the back channel to the video VOD system 402. Then in step 610, the subscriber station 408 receives tuning data indicating both which channel of a plurality of pre-defined VOD channels the content will be transmitted on and which PIDs (program identification numbers) the content will be marked with. The PIDs are selected by the session manager 406 and sent by value or by reference to the server 404 and the subscriber station 408. The sever 404 preferably provides the requested program on an available channel and the PIDs are included in the header of all packets sent on a stream and associated with the program. Then in step 612, the subscriber station 408 tunes to the channel specified by the tuning data from step 610. Next in step 606, the subscriber station 408 receives the scrambled or encrypted VOD service and the de-scrambling message in step 606 responsive the execution of step 510 by the distribution center 104. After step 606, the method continues in step 614. However, prior to step 614, the subscriber station 408 performed step 602 to receive authorization for all VOD service. The subscriber station 408 performs step 602 responsive to step 502, and need perform step 602 only once upon initialization, and long before step 614. Such information would be stored at and by the subscriber station 408. Then in step 614, the subscriber station 408 uses the de-scrambling message, namely the decryption data, to derive or generate the key for de-scrambling the content. Next in step 616, the key is used to de-scramble the VOD service. Finally, in step 618, the subscriber station 408 decodes the signal and displays it the VOD on an associated display device. It should be noted that access to the VOD service is controlled in two ways. First, requiring the key for decryption protects all content of the VOD service. Second, the access to the VOD service for a particular subscriber station 408 is controlled by the VOD

system 402 that controls whether the subscriber station 408 knows which channel is being used to provide the VOD service, thus, to which the subscriber station 408 must tune.

Those skilled in the art will recognize that additional keys may be used to provide additional levels of security. For example, at a later time a second key may be substituted for the first key, where the first key and the second key are both members of a first set of keys, and where the decryption data is usable to decrypt each member of the first set of keys. These and other modifications to the general methods described above with reference to Figures 5 and 6A are contemplated by the present invention.

Referring now to Figure 6B, the case where a subscriber station 408 has not requested video-on-demand services will be described. Figure 6B illustrates the processing that occurs at the subscriber station 408 when no service has been requested. As shown, the subscriber station 408 performs step 602 as do all subscriber stations 408 to become authorized for VOD services. However, since no service has been ordered, the subscriber station 408 will not send a request for VOD service to the VOD system 402 in step 620, and therefore, will also never receive the necessary tuning data in step 622. Thus, any attempts in step 624 to get the VOD service without notifying the video VOD system 402 and thus not be charged is not possible. Figure 6B, most clearly shows that it is the failure to provide tuning data in the present invention that prevents a authorized subscriber station 408 that has not ordered the VOD services from decoding the VOD services signal.

Referring now to Figure 6C, the processing that occurs at the subscriber station 408 when a non-subscriber attempts to pirate video-on-demand services will be described. The non-subscriber by definition will not receive the authorization in step 628. Since the subscriber station 408 is a non-subscriber there will have been no initialization and not received the authorization in step 628. Nonetheless, the non-subscribing station 408 may through illegitimate means determine the tuning data in step 626. Then in step 612, the non-subscribing station 408 could tune to the channel having the VOD services. Next in step 606, the non-subscribing station 408 receives the scrambled VOD services and the de-scrambling message. In step 632, the non-subscribing station 408 will attempt to derive or generate the key, however, it does not have the authorization and data necessary to derive the key, and therefore will be unable to de-scramble the VOD services. Thus, the lack of the authorization and thus the key provides the protection against theft of the VOD services.

The differences between the claimed invention and the prior art are further highlighted by Figures 7 & 8. Each Figure shows the distribution of keys for controlling

access to the video content provided by the distribution center 104. Figure 7 is a block diagram illustrating the transmission of data and keys with respect to the transport stream such as MPEG according to the prior art. As shown in Figure 7, for each program, the prior art sends a different key associated with the program, and thus, controls access to the program. In other words, each subscriber station 408 is enabled to access the program depending on whether the subscriber station 408 has received the key corresponding to the program. In the prior art this is not problematic because there are relatively few programs. In contrast in VOD services, there may be thousands of programs, and if each required a separate key, the distribution of the keys themselves would cause failures making the programs not accessible to the subscriber stations 408. In contrast and as shown in Figure 8, the methods of the present invention do not use the keys to control access to the programs, and do not require a separate key set for each program. As can be seen in Figure 8, a single key or key set is distributed to all subscriber stations. This key or key set is then used for all programs. This greatly reduces the control traffic over the network 106, and is particularly advantageous for VOD services where the thousands of programs requiring a separate key for each subscriber station are not possible.

Referring now to Figure 9, the advantage of the present invention in using one or a smaller set of key is shown. Figure 9 is diagram for a hybrid fiber/coax network 900 including a headend 902, plurality of nodes 904 providing a plurality of channel 906 each having a plurality of programs 908. Figure 9 illustrates the use of the same key for each channel. In such a case, the number of keys to be distributed is reduced by a factor of n. Where n is the number of programs 908 per channel or frequency. In the preferred embodiment for the system described above this an 8:1 reduction in the number of keys needed. Similarly, this concept can be extended to used one key for groups of channel, or even one key for each node. Thus, the present invention ensures that the distribution of keys is not a obstacle to providing the conditional access desired.

Thus, in summary, the present invention uses the mechanisms of (1) scrambling, (2) authorization messages and (3) tuning to control access. The subscriber station 408 requires all three to be able to receive and de-scramble signals transmitted over the network 106 to the subscriber station 408. The present invention, however, minimizes traffic over the network 106 by using the same encryption/decryption keys for the channels; and sending authorization messages upon initialization. Therefore, even though there are thousands of

programs each being sent to individual subscriber, conditional access is maintained with nominal impact on network bandwidth.

It is to be understood that the specific mechanisms and techniques that have been described are merely illustrative of one application of the principles of the invention. For example, while the present invention is described in application to a video on-demand system, it also has some application in other point cast on-demand services such as data. Numerous additional modifications may be made to the methods and apparatus described without departing from the true spirit of the invention.

WHAT IS CLAIMED IS:

1. A method for providing conditional access to video-on-demand services for a plurality of subscriber stations, the method comprising:

sending an authorization message to the plurality of subscriber stations to authorize the plurality of subscriber stations to receive the video-on-demand services;

receiving a first order for a first video service from a first subscriber station; and

transmitting tuning data to the first subscriber station so that the first subscriber station is able to receive the first video service.

2. The method of claim 1, further comprising the steps of:

scrambling the first video service using a first key to generate a first scrambled video service;

scrambling the first key to generate a first scrambled key;

transmitting the first scrambled video service to the plurality of subscriber stations;

transmitting the first scrambled key to the plurality of subscriber stations.

3. The method of claim 2, wherein the authorization message further comprises data to derive the first scrambled key to the plurality of subscriber stations.

4. The method of claim 3 wherein the control message is an entitlement control message.

5. The method of claim 3 wherein the de-scrambling message is an entitlement control messages.

6. The method of claim 1, wherein the step of transmitting tuning data includes transmitting a service frequency and a MPEG program number by value or reference.

7. The method of claim 1, wherein the video services comprise video on-demand services.

8. The method of claim 1, wherein the video services are distributed by way of a video distribution system from the group of video distribution systems including a cable

distribution network, a satellite system, a digital subscriber line system, and a microwave system.

9. The method of claim 2, wherein at a later time a second key is substituted for the first key, where the first key and the second key are both members of a first set of keys, and where the decryption data is usable to decrypt each member of the first set of keys.

10. A method for providing conditional access to video-on-demand services to a subscriber station in a video-on-demand (VOD) system, the method comprising the step of:

receiving an authorization message at the subscriber station from the VOD system;

sending a signal to request a video service from the subscriber station to the VOD system; and

receiving tuning data at the subscriber station;

using the tuning data to tune to the video service; and

receiving the video service and displaying it on display device.

11. The method of claim 10, wherein the step of receiving the video service further comprises the steps of:

receiving and de-scrambling a encryption/decryption key;

de-scrambling the video service using the encryption/decryption key; and

providing an unscrambled video service.

12. The method of claim 11, where in the step of receiving an authorization message further comprises the steps of:

receiving a control message for the subscriber station that includes an instruction to de-scramble the encryption/decryption key; and

receiving a de-scrambling message that includes data to derive the encryption/decryption key.

13. The method of claim 12 wherein the control message is an entitlement control messages.

14. The method of claim 12 wherein the de-scrambling message is an entitlement control messages.

15. The method of claim 1, wherein the step of receiving tuning data includes receiving a service frequency and a MPEG program number by value or reference.

16. The method of claim 15, wherein the step of using the tuning data to tune to the video service comprises the step of setting a de-multiplexer to receive on the service frequency and extract packets matching the MPEG program number.

17. The method of claim 11, wherein at a later time a second key is substituted for the first key, where the first key and the second key are both members of a first set of keys, and where the decryption data is usable to decrypt each member of the first set of keys.

18. A method for conditionally accessing video services, the method comprising:
transmitting an order for a first video service;
receiving tuning data;
using the tuning data to tune to the first video service;
receiving an scrambled version of the first video service; and
receiving an scrambled version of a first key for decrypting the scrambled version of the first video service.

19. The method of claim 18, the method further comprising:
receiving decryption data for decrypting the scrambled version of the first key;
decrypting the scrambled version of the first key using the decryption data to generate the first key; and
decrypting the scrambled version of the first video service using the first key to generate the first video service.

20. The method of claim 18, wherein the video services comprise video on-demand services.

21. The method of claim 18, wherein the video services are distributed by way of a cable distribution network.

22. The method of claim 21, wherein the method is performed at a subscriber station coupled to the cable distribution network.

23. The method of claim 18, further comprising receiving authorization for the video services.

24. The method of claim 19, wherein the decryption data is received by way of an entitlement control message.

25. The method of claim 19, wherein at a later time a second key is substituted for the first key, where the first key and the second key are both members of a first set of keys; and where the decryption data is usable to decrypt each member of the first set of keys.

26. A video-on-demand system providing conditional access to video services, the system comprising:

a video-on-demand system for providing video content, tuning information and access control messages;

a distribution network coupled to the video-on-demand system for transmitting video content, tuning information and access control messages, the distribution network coupled to the video-on-demand system; and

a plurality of subscriber stations being coupled to the distribution network to receive video content, tuning information and access control messages, the subscriber station tuning to a frequency and de-scrambling video content in responsive to access control messages from the video-on-demand system.

27. The system of claim 26, wherein the video-on-demand system further comprises:

a content server for storing and providing video content;

a multiplexer/scrambler for multiplexing a plurality of signal and generating video streams, the multiplexer/scrambler coupled to the content server and responsive to control signals; and

a session manager for controlling the video content provided by the content server and its transmission, the session manage coupled to the video content server and the multiplexer/scrambler.

28. The system of claim 26, further comprising a conditional access system coupled to the session manager and the multiplexer/scrambler, the conditional access system providing control signals, encryption keys and authorization messages to the multiplexer/scrambler in response to signals from the session manager.

29. The system of claim 28, wherein the conditional access system uses ECM to send control signals to the subscriber stations.

30. The system of claim 28, wherein the conditional access system uses the same ECM having the same key for the plurality of subscriber stations.

31. The system of claim 28, wherein the conditional access system provides an authorization message to each subscriber stations upon initialization to enable access to and de-scrambling of the video service.

32. The system of claim 27, wherein the session manager controls the frequency and program ID for the video content provided the distribution network.

33. The system of claim 26, wherein the subscriber station further comprises:

a de-multiplexer coupled to the distribution network to receive the video content;

a key generator for producing a key and coupled to the de-multiplexer to receive an ECM;

a de-scrambler coupled to the key generator and the de-multiplexer, the de-scrambler decrypting a signal from the de-multiplexer to generate the video content; and

a controller coupled to VOD system to receive control signals, the controller coupled to the key generator to provide an EMM and the de-multiplexer to provide tuning information.

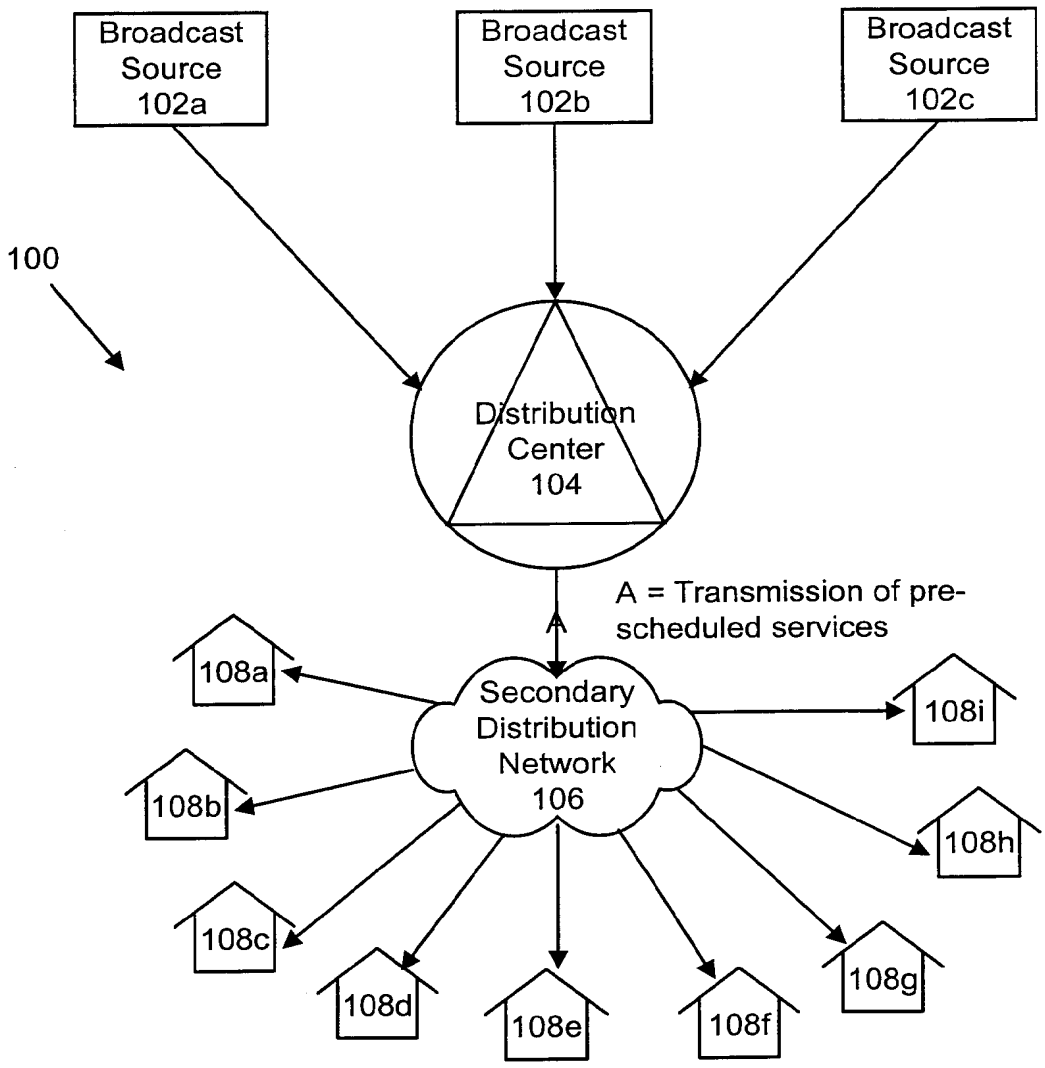


Figure 1 (Prior Art)

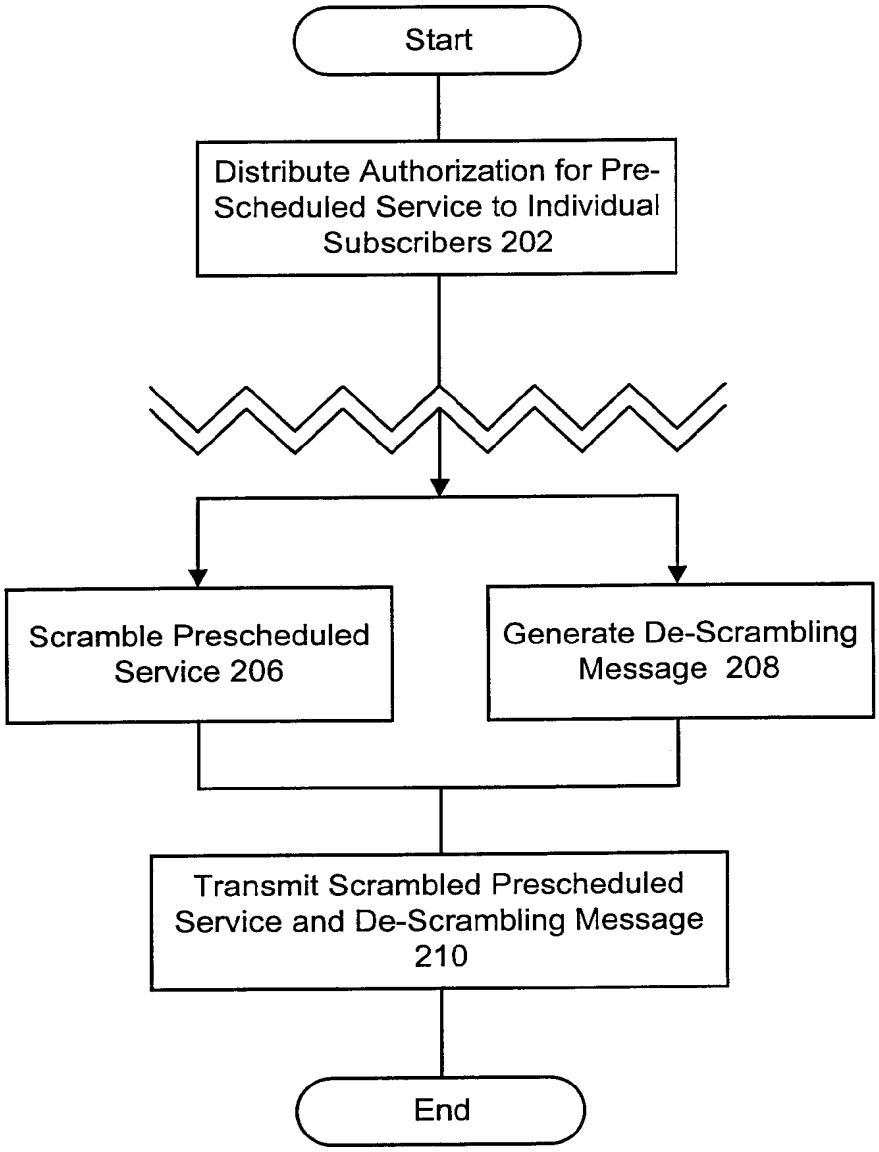


Figure 2 (Prior Art)

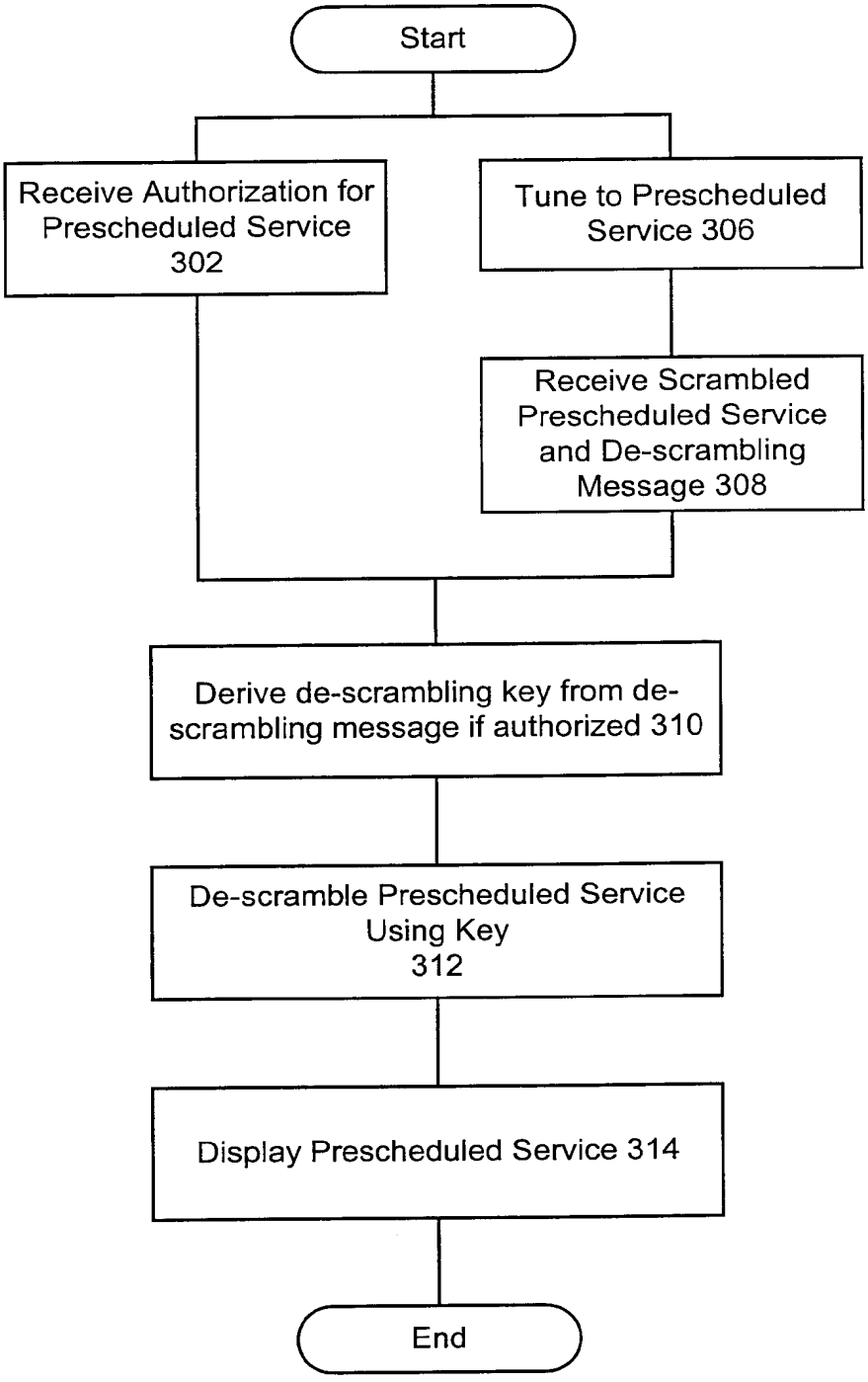


Figure 3A (Prior Art)

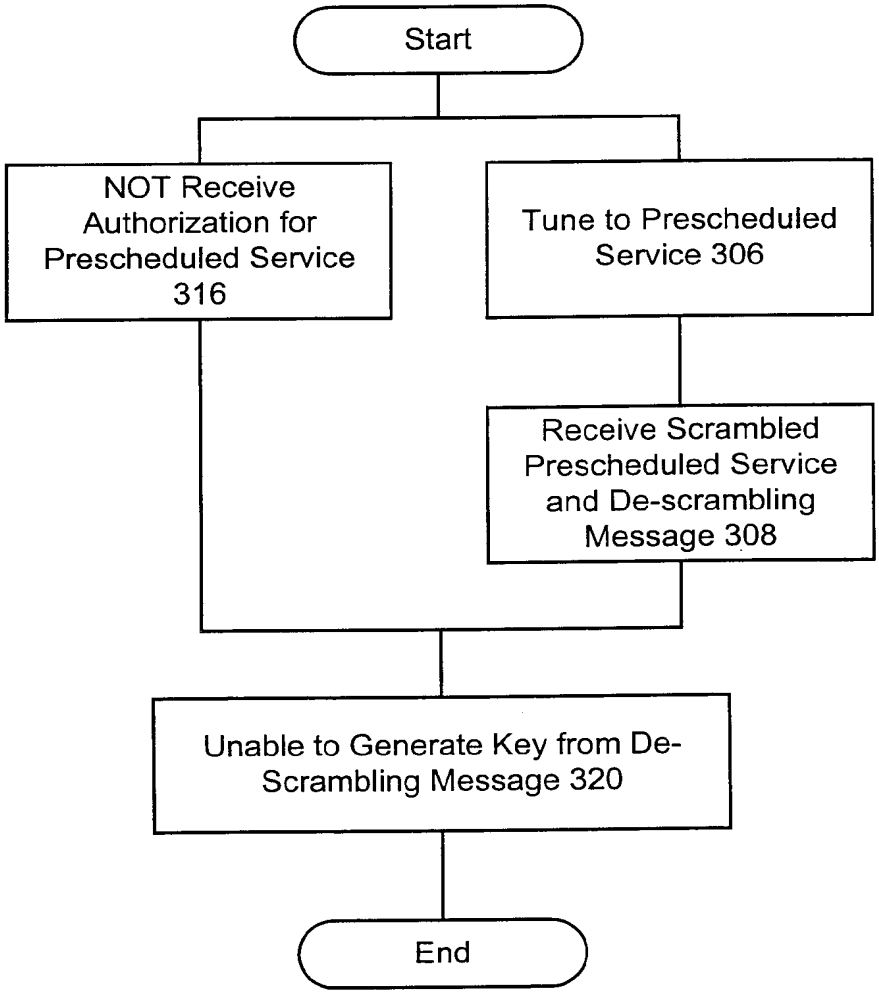


Figure 3B (Prior Art)

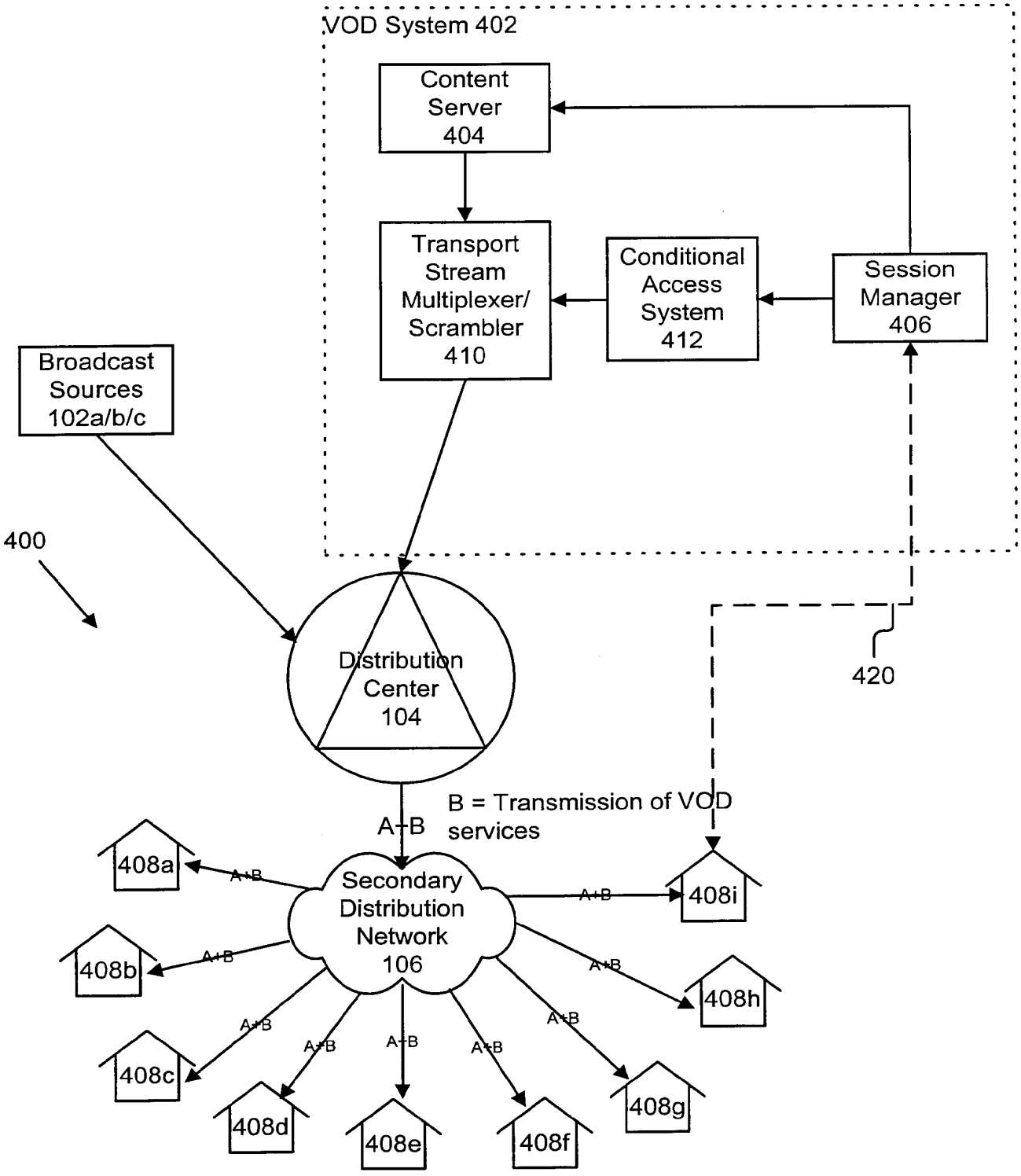

VOD System 402
Content Server 404
Transport Stream Multiplexer/ Scrambler 410
Conditional Access System 412
Session Manager 406
Broadcast Sources 102a/b/c
400
Distribution Center 104
420
A+B
B = Transmission of VOD services
Secondary Distribution Network 106
408a
408b
408c
408d
408e
408f
408g
408h
408i

Figure 4A

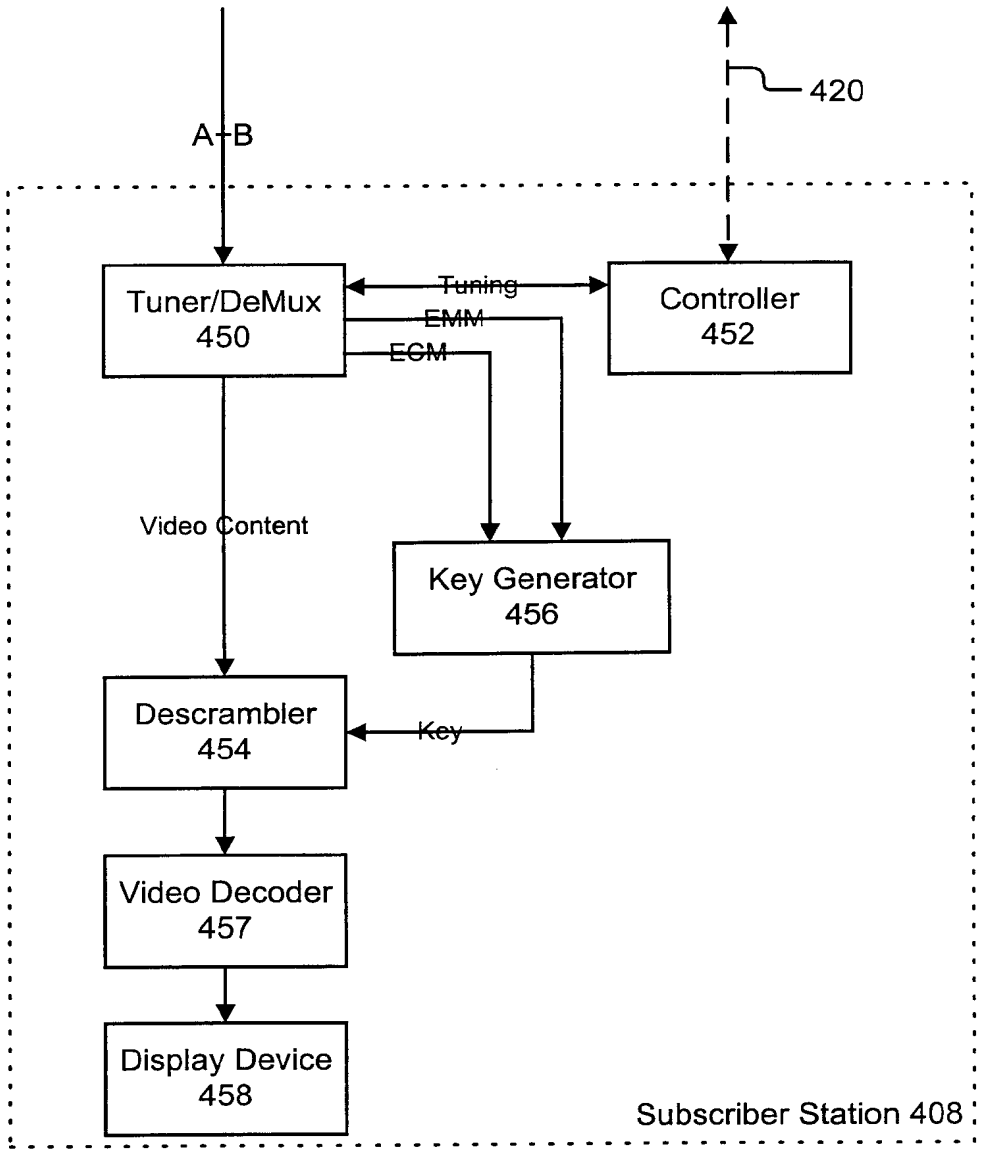

A-B
420
Tuner/DeMux
450
Tuning
EMM
ECM
Controller
452
Video Content
Key Generator
456
Descrambler
454
Key
Video Decoder
457
Display Device
458
Subscriber Station 408

Figure 4B

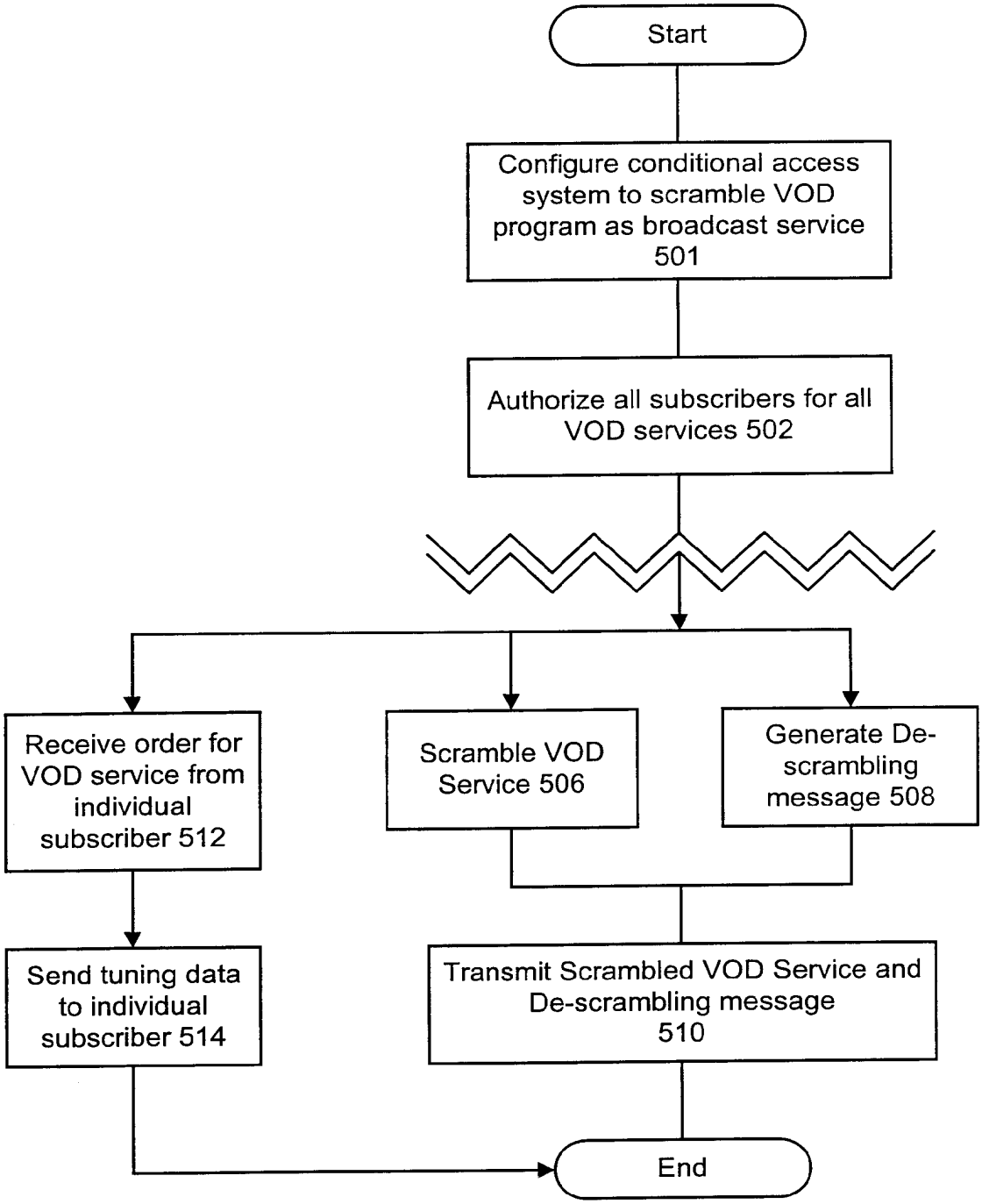

Start
Configure conditional access system to scramble VOD program as broadcast service 501
Authorize all subscribers for all VOD services 502
Receive order for VOD service from individual subscriber 512
Scramble VOD Service 506
Generate De-scrambling message 508
Send tuning data to individual subscriber 514
Transmit Scrambled VOD Service and De-scrambling message 510
End

Figure 5

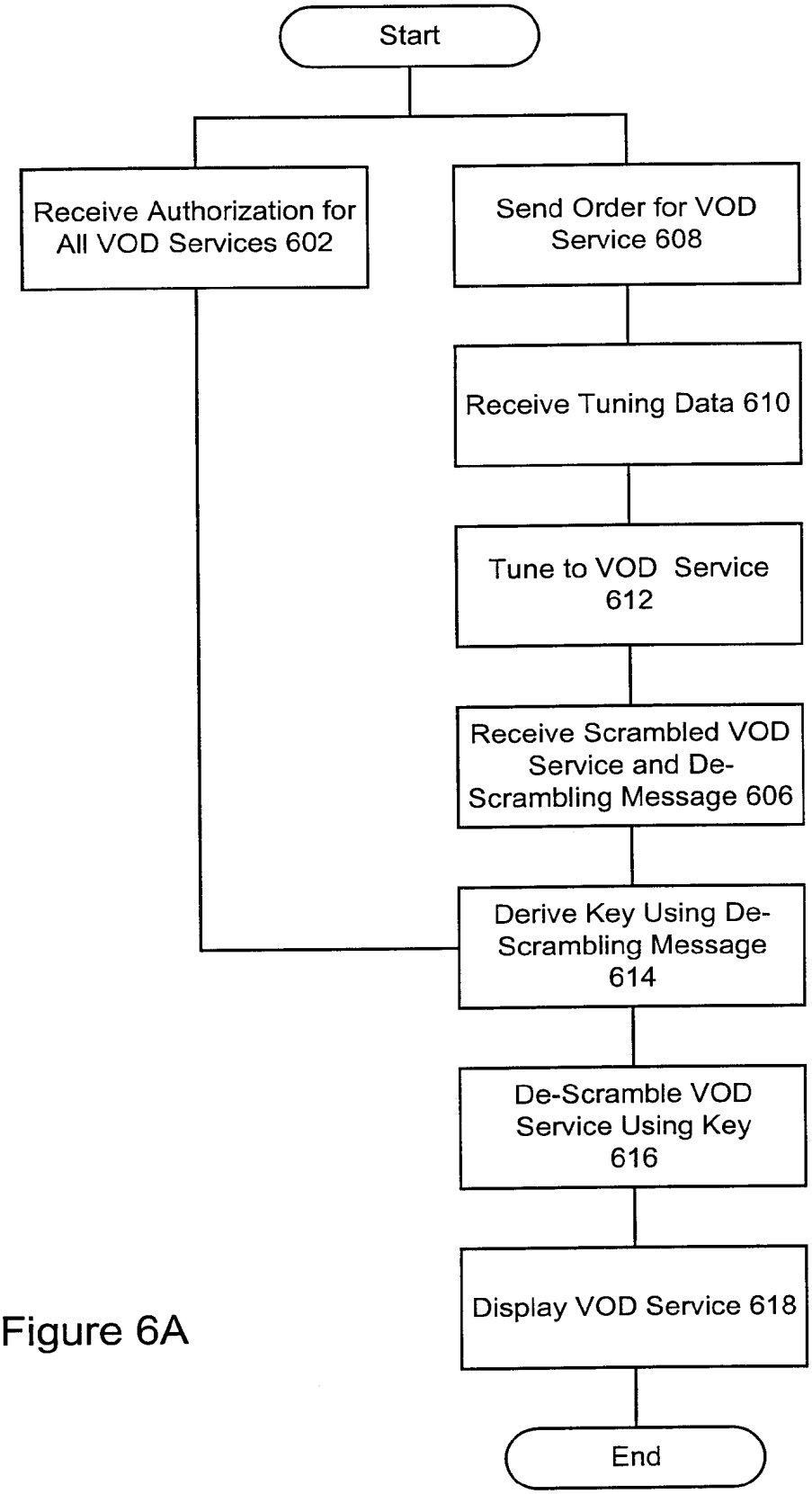

Start
Receive Authorization for All VOD Services 602
Send Order for VOD Service 608
Receive Tuning Data 610
Tune to VOD Service 612
Receive Scrambled VOD Service and De-Scrambling Message 606
Derive Key Using De-Scrambling Message 614
De-Scramble VOD Service Using Key 616
Display VOD Service 618
End

Figure 6A

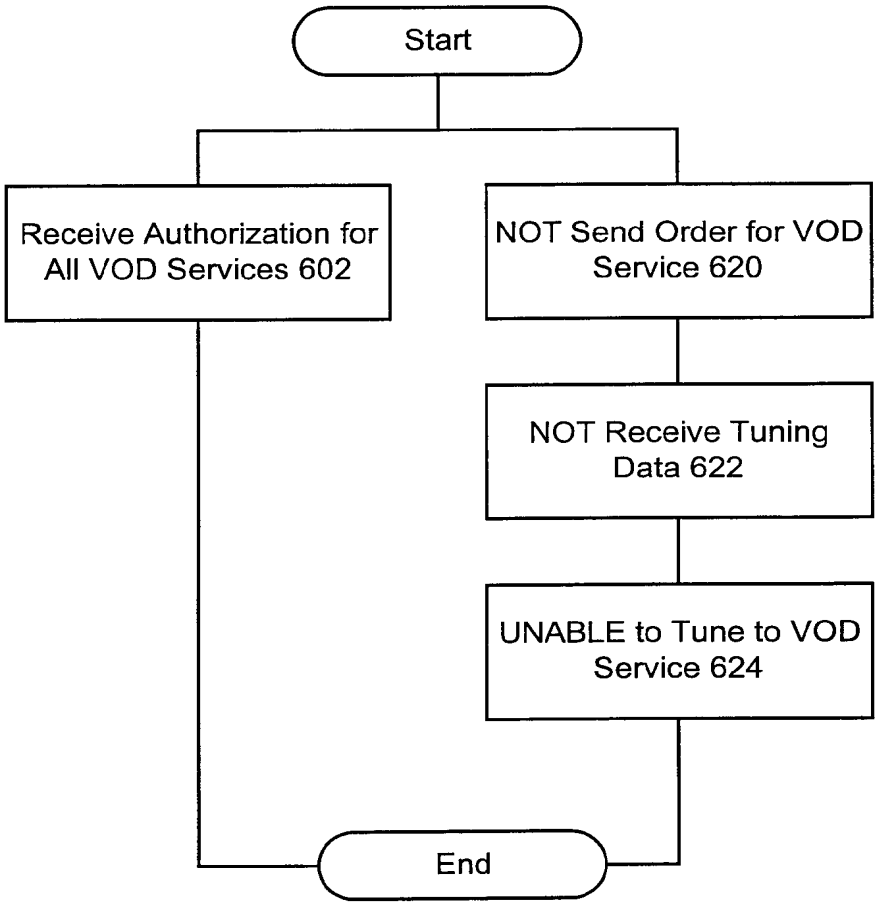

Start
Receive Authorization for All VOD Services 602
NOT Send Order for VOD Service 620
NOT Receive Tuning Data 622
UNABLE to Tune to VOD Service 624
End

Figure 6B

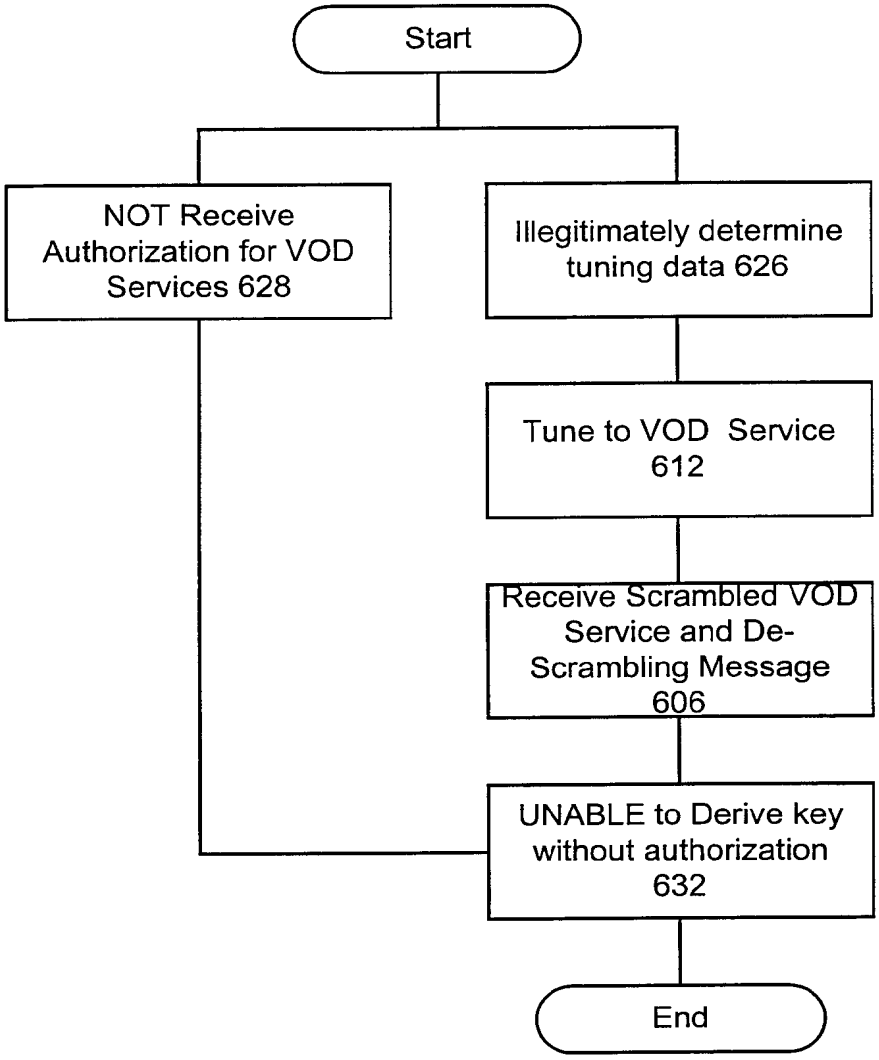

Start
NOT Receive Authorization for VOD Services 628
Illegitimately determine tuning data 626
Tune to VOD Service 612
Receive Scrambled VOD Service and De-Scrambling Message 606
UNABLE to Derive key without authorization 632
End

Figure 6C

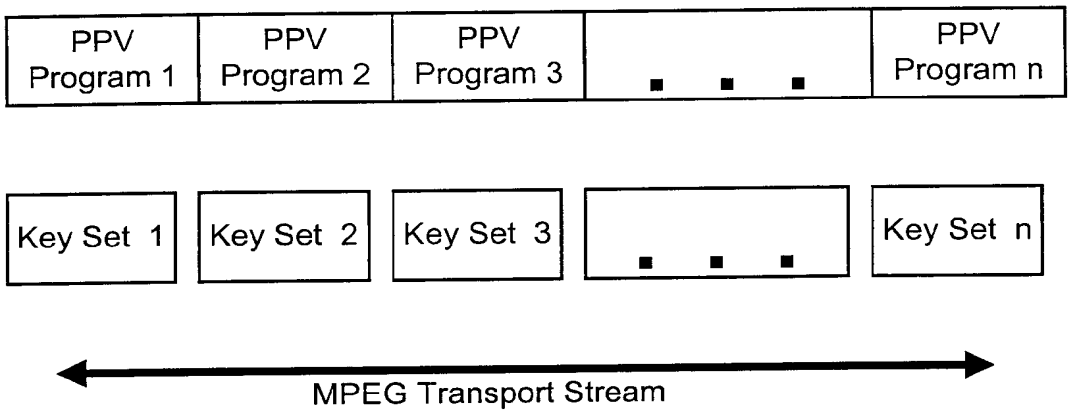


Figure 7 (Prior Art)

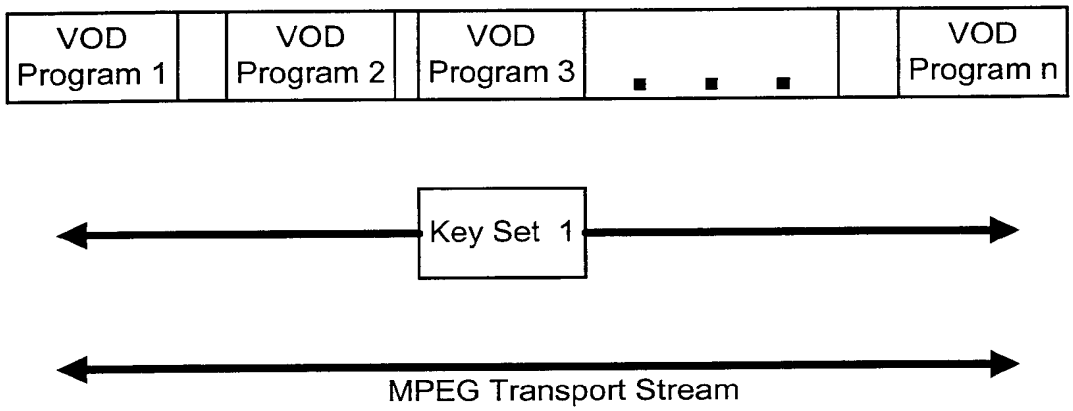

VOD Program 1
VOD Program 2
VOD Program 3
VOD Program n
Key Set 1
MPEG Transport Stream

Figure 8

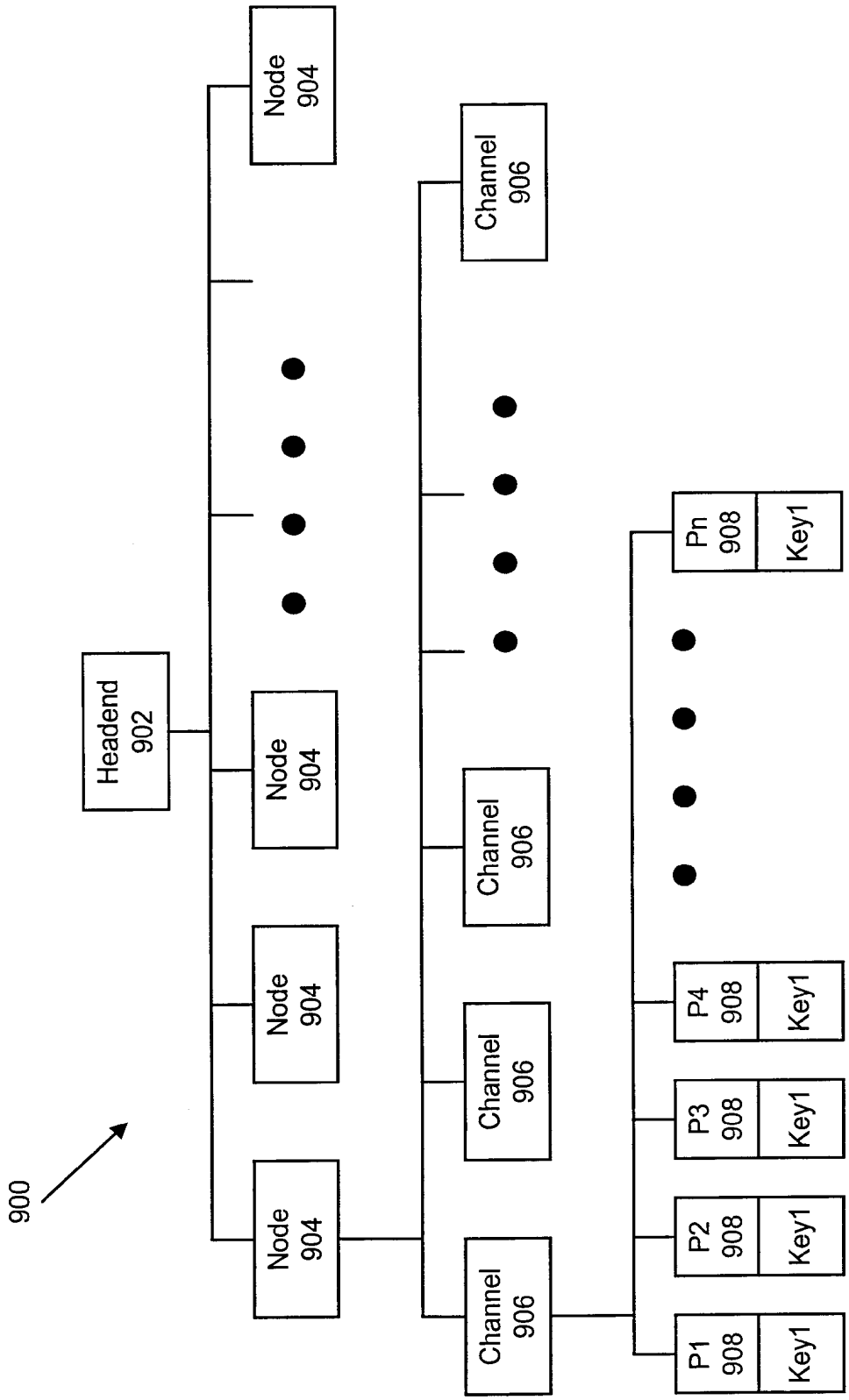

900
Headend 902
Node 904
Node 904
Node 904
Node 904
Channel 906
Channel 906
Channel 906
Channel 906
P1 908
Key1
P2 908
Key1
P3 908
Key1
P4 908
Key1
Pn 908
Key1

Figure 9

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 01/01173

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 4 430 669 A (CHEUNG WILLIAM S H) 7 February 1984 (1984-02-07) the whole document	1,10,18, 26 2-9, 11-17, 19-25, 27-33
Y A	WO 99 16247 A (SARNOFF CORP) 1 April 1999 (1999-04-01) the whole document	1,10,18, 26 2-9, 11-17, 19-25, 27-33
A	US 4 736 422 A (MASON ARTHUR G) 5 April 1988 (1988-04-05) column 1, line 1 - line 66	1-33

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 April 2001	08/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Greve, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 01/01173

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 247 364 A (BACON KINNEY C ET AL) 21 September 1993 (1993-09-21) column 1, line 15 -column 2, line 4	1-33
A	PATENT ABSTRACTS OF JAPAN vol. 010, no. 121 (E-401), 7 May 1986 (1986-05-07) & JP 60 253386 A (TOSHIBA KK), 14 December 1985 (1985-12-14) abstract	1-33
A	US 4 866 770 A (SETH-SMITH NIGEL ET AL) 12 September 1989 (1989-09-12) abstract	1-33

INTERNATIONAL SEARCH REPORT

Interna .ial Application No
PCT/US 01/01173

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4430669 A	07-02-1984	NONE	
WO 9916247 A	01-04-1999	US 6118498 A	12-09-2000
		AU 9585498 A	12-04-1999
		AU 9588198 A	12-04-1999
		AU 9588298 A	12-04-1999
		AU 9670698 A	12-04-1999
		AU 9778898 A	12-04-1999
		EP 1025537 A	09-08-2000
		EP 1025709 A	09-08-2000
		EP 1025697 A	09-08-2000
		EP 1055325 A	29-11-2000
		EP 1025692 A	09-08-2000
		US 5933195 A	03-08-1999
		US 6122400 A	19-09-2000
		US 6057889 A	02-05-2000
		US 6118486 A	12-09-2000
		US 5987180 A	16-11-1999
		WO 9916011 A	01-04-1999
		WO 9916243 A	01-04-1999
		WO 9916242 A	01-04-1999
		WO 9916012 A	01-04-1999
		WO 9916253 A	01-04-1999
		WO 9916235 A	01-04-1999
US 4736422 A	05-04-1988	AT 37762 T	15-10-1988
		DE 3474496 D	10-11-1988
		EP 0148235 A	17-07-1985
		WO 8500491 A	31-01-1985
		JP 5021397 B	24-03-1993
		JP 60501883 T	31-10-1985
		AT 33739 T	15-05-1988
		DE 3470646 D	26-05-1988
		EP 0151147 A	14-08-1985
		WO 8500718 A	14-02-1985
		JP 5025436 B	12-04-1993
		JP 60501882 T	31-10-1985
		US 4802215 A	31-01-1989
US 5247364 A	21-09-1993	AU 3222693 A	28-06-1993
		WO 9311638 A	10-06-1993
		US 5497187 A	05-03-1996
JP 60253386 A	14-12-1985	NONE	
US 4866770 A	12-09-1989	AT 113782 T	15-11-1994
		AU 606354 B	07-02-1991
		AU 7850587 A	08-03-1988
		DE 3750724 D	08-12-1994
		DE 3750724 T	23-03-1995
		DK 198788 A	14-06-1988
		EP 0318507 A	07-06-1989
		FI 890683 A,B,	13-02-1989
		JP 2500477 T	15-02-1990
		JP 2752979 B	18-05-1998
		NO 173630 C	05-01-1994
		WO 8801463 A	25-02-1988
		US 4890321 A	26-12-1989